REMARKS

The Office Action dated January 22, 2009, has been received and carefully noted. The above amendments to the claims, and the following remarks, are submitted as a full and complete response thereto.

Claims 1-2, 5-9, 12-18, 21-25, 28-34, 37-40, and 43-44 are currently pending in the application, of which claims 1, 8, 15, 17, 24, 31, 33, and 39 are independent claims. Claims 1, 8, 15, 17, 24, 31, 33, and 39 have been amended to more particularly point out and distinctly claim the invention. No new matter has been added. Claims 1-2, 5-9, 12-18, 21-25, 28-34, 37-40, and 43-44 are respectfully submitted for consideration.

The specification was rejected to as failing to provide proper antecedent basis for the claimed subject matter. Specifically, the Office Action alleged that the specification fails to define the term, "computer readable medium." The claims have been amended, rendering this objection moot. Withdrawal of the objection is respectfully requested, as the specification provides either clear support or antecedent basis for the recitations in the claims.

The Office Action rejected claims 17, 18, 21-25, and 28-30 under 35 U.S.C. §101 as allegedly directed to non-statutory subject matter. Specifically, the Office Action alleged that the term, "computer readable medium," recited in the claims, could be construed to include signals. Presently pending claims 17 and 24 recite "computer-readable storage medium," which it is respectfully submitted cannot reasonably be considered to include signals. Withdrawal of the rejection is respectfully requested.

Claims 1, 5-6, 8, 12-13, 15, 17, 24, 28-29, 31, 33, 37, 39, and 42-43 were rejected under 35 U.S.C. §103(a) as being allegedly unpatentable as obvious over U.S. Patent No. 6,968,349 of Owen *et al.* ("Owen") in view of U.S. Patent No. 4,864,616 of Pond *et al.* ("Pond"). The Office Action acknowledged that Owen does not disclose or suggest all of the features of the claims. The Office Action, therefore, cited Pond to remedy the deficiencies of Owen. Applicants respectfully traverse this rejection.

Claim 1, upon which claims 2 and 5-6 depend, is directed to a method including receiving a second data record to be stored on a single database, wherein the database comprises a first data record. The method also includes storing the second data record on the database, wherein the second data record is stored consecutive to the first data record. The method further includes retrieving a first integrity checksum stored with the first data record previous to the second data record. The method additionally includes computing a second integrity checksum for the second data record with a cryptographic method using a storage key, the retrieved first integrity checksum and the second data record. The method also includes storing the second integrity checksum on the database. The method further includes configuring the retrieved integrity checksum for a first row of the database to be a generated initialization vector or a digital signature of a signing entity.

Claim 8, upon which claims 9 and 12-14 depend, is directed to a method including retrieving a second data record to be verified from a single database. The method also includes retrieving a second integrity checksum of the second data record, wherein the first data record and the second data record are consecutive data records in the database.

The method further includes retrieving a first integrity checksum of the first data record previous to the retrieved second data record. The method additionally includes computing a third integrity checksum for the second data record using the retrieved second data record, the first integrity checksum, and a storage key. The method also includes comparing the second integrity checksum to the third integrity checksum, wherein the second data record is considered authentic when the second integrity checksum and the third integrity checksums are equal. The method further includes configuring the retrieved integrity checksum for a first row of the database to be a generated initialization vector or a digital signature of a signing entity.

Claim 15, upon which claim 16 depends, is directed to a system including a single database configured to store and provide signed data. The system also includes a data source configured to provide data records to be stored on the database. The system further includes a signing entity configured to sign data records to be stored on the database system with a second integrity checksum computed using a second data record, a first integrity checksum of the first data record previous to the second data record to be signed, and a storage key, wherein the first data record and the second data record are consecutive data records in the database. The system additionally includes a verification entity configured to verify integrity of chosen data records by computing a computed third integrity checksum using the second data record, the first integrity checksum of the first data record previous to the second data record, and the storage key, and comparing the computed third integrity checksum to the second integrity checksum stored on the database.

Claim 17, upon which claims 18 and 21-23 depend, is directed to a computer program embodied on a computer-readable storage medium, wherein the computer program performs a process when executed in a computer device. The process includes receiving a second data record to be stored on a single database, wherein the database comprises a first data record. The process also includes storing the second data record on the database, wherein the second data record is stored consecutive to the first data record. The process further includes retrieving a first integrity checksum stored with the first data record previous to the second data record. The process additionally includes computing a second integrity checksum for the second data record with a cryptographic method using a storage key, the retrieved first integrity checksum and the second data record. The process also includes storing the second integrity checksum on the database. The process further includes configuring the retrieved integrity checksum for a first row of the database to be a generated initialization vector or a digital signature of a signing entity.

Claim 24, upon which claim 25 and 28-30 depend, is directed to a computer program embodied a computer-readable storage medium, wherein the computer program performs a process when executed in a computer device. The process includes retrieving a second data record to be verified from a database. The process also includes retrieving a second integrity checksum of the second data record to be verified from a database. The process further includes retrieving a first integrity checksum of a first data record previous to the retrieved second data record, wherein the first data record and the second data record are consecutive data records in the database. The process additionally includes computing a third integrity checksum for the second data record using the retrieved second data record, the first integrity checksum, and a storage key. The process also includes comparing the second integrity checksum to the third integrity checksum, wherein the second data record is considered authentic when the second integrity checksum and the third integrity checksums are equal. The process further includes configuring the retrieved integrity checksum for a first row of the database to be a generated initialization vector or a digital signature of a signing entity.

Claim 31, upon which claims 32 depends, is directed to a system including storage means for storing and providing signed data, wherein the storage means is singular. The system also includes provision means for providing data records to be stored on the storage means. The system further includes signing means for signing data records to be stored on the storage means with a second integrity checksum computed using a second data record, a first integrity checksum of the first data record previous to the second data record to be signed, and a storage key, wherein the first data record and the second data record are consecutive data records in the database. The system additionally includes verification means for verifying integrity of chosen data records by computing a computed third integrity checksum using the second data record, the first integrity checksum of the first data record previous to the second data record, and the storage key, and comparing the computed third integrity checksum to the second integrity checksum stored on the storage means.

Claim 33, upon which claims 34 and 37-38 depend, is directed to an apparatus including a receiver configured to receive a second data record to be stored on a single database, wherein the receiver is further configured to receive a first integrity checksum stored with a first data record previous to the second data record, wherein the first data record and the second data record are consecutive data records in the database. The apparatus also includes a processor configured to compute a second integrity checksum for the second data record with a cryptographic method using a storage key, the received first integrity checksum and the second data record. The apparatus further includes a memory configured to store the second data record and the second integrity checksum on the database, wherein the second data record is stored consecutive to the first data record. The retrieved integrity checksum for a first row of the database is configured to be a generated initialization vector or a digital signature of a signing entity.

Claim 39, upon which claims 40 and 43-44 depend, is directed to an apparatus including a receiver configured to receive a second data record to be verified from a single database, wherein the receiver is also configured to receive a second integrity checksum of the second data record, wherein the first data record and the second data record are consecutive data records in the database, and wherein the receiver is further configured to receive a first integrity checksum of a first data record previous to the received second data record. The apparatus also includes a processor configured to compute a third integrity checksum for the second data record using the received second data record, the first integrity checksum, and a storage key, wherein the processor is further configured to compare the second integrity checksum to the third integrity checksum, wherein the second data record is considered authentic when the second integrity checksum and the third integrity checksums are equal. The retrieved integrity checksum for a first row of the database is configured to be a generated initialization vector or a digital signature of a signing entity.

Applicants respectfully submit that the combination of Owen and Pond fails to disclose or suggest all of the elements of any of the presently pending claims.

Owen generally relates to an apparatus and method for validating a database record before applying journal data. Owen discusses a system relating to journaling databases. In principle a journaling database is a database that logs changes to a journal (usually a circular log in a specially-allocated area) before actually writing them to the main database. Such databases are less likely to become corrupted in the event of power failure or system crash.

At column 1, lines 39-47, Owen defines what a data journal of Owen is. "Most journals known in the art record all fields in a record before a change is made to the record, including fields in the record that do not change. Because recording data that has not changed takes valuable space and time in a database journal, a newer concept known as minimized data journaling was introduced. With a minimized data journal, only the changed fields of a record are recorded, which assumes that the fields in the record that are not represented in the journal did not change."

Before a detailed discussion of those features, it must be noted that a fundamental differences is that journal entries always relate to changes made in the database. Certain embodiments of the present invention are designed for preventing any changes except adding a new complete record with corresponding integrity check sum. These two elements are always new information that cannot be derived from modifications of the earlier data.

First feature: it is said in the Office Action that "retrieving a second data record to be verified from the single database," as recited in claim 8, corresponds to "the minimized data journal entry is read," as allegedly taught in Owen. These two things are not the same because the second data record (as claimed) is a complete data record and not a minimized journal entry, as the term "data record" would be interpreted by one of ordinary skill in the art, reading the claim in light of the specification without importing limitations from the specification into the claims.

As best understood, the Office Action has interpreted the minimized journal entry as data records, just not complete data records, and has interpreted the claims as not requiring complete data records, since the word "complete" is not specifically set forth in the claims. Applicants respectfully note, however, that the minimized journal entries would not be viewed as data records at all (neither complete nor incomplete data records) in the view of one of ordinary skill in the art. Instead, they would be viewed as items that are associated with a data record. This can be seen from Owen itself, which distinguishes between a "record" and a "journal entry." Unless the USPTO can provide evidence that one of ordinary skill in the art would also consider the journal entries to be "records," it is respectfully submitted that all of the evidence of record supports only Applicants' conclusion that a minimized journal entry is not a data record (whether complete or not) as recited in the claims. Withdrawal of the rejection is respectfully requested on at least this basis.

Second feature: it is said in the Office Action that "retrieving a second integrity checksum," as recited in claim 8, corresponds to a redundancy check. The checksum (as claimed), however, is used only for checking the **integrity** of the data record. Integrity is not same as redundancy. Integrity means that the contents of the records must not have been altered to any changes and the records must be in the same order as they were stored. Then, it is said in the Office Action that "when the minimized data journal entry is to be applied to the corresponding database record, a validation value for the record is first **computed** using the same algorithm used to compute the validation value stored in the journal entry." (emphasis added) In the cited step of the method, however, nothing is computed but the integrity checksum is retrieved from the database. Thus, the alleged correspondence is improper.

As best understood, the Office Action has taken the position that the Cyclic Redundancy Check (CRC) in effect does determine the integrity of a data record. Even assuming (for the sake of the argument) that this is an acceptable interpretation, the

Office Action has not identified a second integrity checksum being **retrieved**. Instead, the second alleged integrity checksum is simply computed in Owen. Thus, even assuming the "integrity" limitation were met (for the sake of the argument), still the "retrieving" feature would not be met.

Third feature: the Office Action indicated that "retrieving a first integrity checksum" (as recited in claim 8) corresponds to "the validation value comprises a checksum that is computed using both the data in the old record and the metadata for the old record," as allegedly taught in Owen. This has a similar problem to the previous argument, as nothing is computed in the recited step of retrieving and nothing is retrieved in the cited portion of Owen.

Furthermore, if this portion of the claim is so interpreted, the old record of Owen must (under the Office Action's interpretation) correspond to the first data record of the claims. In the claims, however, the second integrity checksum would then have to be computed using the old record (first integrity checksum) **and** the current record (second data record). Thus, the computation recited in the presently pending claims is not anticipated by Owen.

Fourth feature: This is actually the only feature in the claim that expressly recites "computing" ("computing a third integrity checksum" as recited in claim 8). It is said, in the Office Action, that the computing is similar to the one that was disclosed with reference to the third feature (above). However, as discussed above, the computation is not the same. Furthermore, the computation is not similar in any meaningful or "obvious" way. Instead, the computation is simply and entirely different.

To provide a specific example, the third integrity checksum is calculated using a retrieved second data record, a first integrity checksum, and "**a storage key**." (claim 8 – emphasis added) There does not appear to be any disclosure in Owen corresponding to this feature, since it does not appear that the CRCs of Owens are computed using any storage key.

Fifth feature: The Office Action stated that the comparison ("comparing the second integrity checksum to the third integrity checksum ..." as recited in claim 8) is same as "If the two validation values match, we know with a high level of confidence that the record is in the identical state it was in just before the changes reflected in the journal entry were made," as allegedly taught in Owen. In claims 8, 15, 24, and 31 there is, however, no mechanism recited for making changes. The whole purpose of certain embodiments of the technology disclosed in these claims is to verify that changes have not been made at all. Thus, Owen's disclosure is not an obvious variant of what is claimed, it is a completely different technology.

Furthermore, in certain embodiments of the present invention, these applications of the invention to prevent changes from being made provide a critical and non-obvious advantage in applications such as banking, where the integrity of the data is important. It is respectfully submitted that Owen leads one of ordinary skill in the art away from the claimed invention and away from the critical and unobvious advantages achieved by certain embodiments of the present invention. The purpose of the journaling database of Owen is to facilitate changes, whereas, in certain embodiments, the purpose of the present invention is to prevent the changes in the database.

Older conventional database managers record all bytes in a record into a log when a change is made to the record, including bytes in the record that do not change. Because recording data that has not changed takes valuable space and time in a database journal, a newer concept known as minimized data journaling was introduced. With a minimized data journal, only the changed bytes of a record are recorded without respect to field boundaries, which assume that the bytes in the record that are not represented in the journal entry did not change. A minimized data journal is generally likely to achieve significantly better performance than a full data journal. Note, however, that this increase in performance comes at a usability cost.

Because a journal entry in a minimized data journal only includes the bytes that changed, the resulting journal entry is in a compressed format that may no longer be easily read, understood, and recognized by a human or auditing program. While this is not a concern in some settings, it may be a significant concern in other settings that require auditing, debugging, or human viewing of database changes.

It is mentioned in the description of the present application that certain embodiments of the present invention are beneficial for databases having logfiles and bank transactions. These lines are in human readable form. Thus, a system using minimized journals is not suitable for the purpose as it does not provide a database that is firstly human readable and secondly cannot be changed.

The Office Action cited column 10, lines 8-27, of Owen. In that section, it is explicitly mentioned that "A validation value is computed that uniquely represents the state of a record before changes are made to the record." Again, the purpose of certain embodiments of the present invention is to prevent the changes.

Then Owen continues "When the minimized data journal entry is to be applied to the corresponding database record, a validation value for the record is first computed using the same algorithm used to compute the validation value stored in the journal entry. If the two validation values match, we know with a high level of confidence that the record is in the identical state it was in just before the changes reflected in the journal entry were made. By validating a database record before applying a change in a journal entry, the preferred embodiments solve the potential problems in the prior art ... ."

This section of Owen indicated that there is not a first record and a second record but only the first record and a change that is desired to be made to the first record. After the change there is an altered first record, not two different records as recited in the present claims. The validation checksum is always computed from the first record and it is only carried with the minimized journal entry in Owen. The purpose of the validation checksum of Owen is to provide certainty that the record was not changed while the modifications are done. In other words, only one person at time may make modifications to that record.

Thus, in certain embodiments of the present invention the first data record is not changed and no journals or other modifications are applied to the data records. Instead sequential records are created, and the integrity (including content and order) of the records can (in certain embodiments) be maintained through the claimed techniques involving a variety of specifically computed checksums that interrelate the records.

Thus, one benefit gained by the use of certain embodiments of the method according to claim 1 is that if the records are stored according to the method, not only the contents of the records but also the order of the records cannot be changed.

Furthermore, Applicants respectfully stress that "computing a second integrity checksum for the second data record with a cryptographic method using a storage key, **the retrieved first integrity checksum**, and the second data record" (claim 1, emphasis added) is not disclosed by Owen. That is to say, there is no second checksum of Owen that is calculated based on a first checksum of Owen. Thus, there is nothing in Owen that can correspond to at least this feature of claim 1 (or the similar features of the other independent claims). This feature can help to link the records together (since the first integrity checksum is of the first data record) and can help prevent a reordering of the data records, including insertion of data records that do not belong in the order. This entire concept (and consequently any mechanisms for achieving such a concept) is entirely missing from Owen.

In short, Owen does not disclose a system similar to the present invention as recited in the presently pending claims. The only arguably common feature (not an admission of relevance) is that both are related to databases. The purpose of the present invention (in various disclosed embodiments) is completely different and the mechanisms for providing the solution for the problems of the cited art are completely different.

Applicants note that Pond was also recited with reference to the rejected claims. Pond, however, has only been cited with respect to other features of the claims. Pond generally relates to cryptographic labeling of electronically stored data. Specifically, the Office Action alleged that Pond discloses "a method wherein an initialization vector is used to derive a checksum." Even assuming this is the case for the sake of the argument, Pond would not (and does not) disclose the other five features discussed above with respect to the independent claims. Thus, Pond does not remedy the above-identified deficiencies of Owen and the combination of Owen and Pond fails to disclose or suggest all of the elements of any of the presently pending claims. Thus, it is respectfully submitted that each of independent claims 1, 8, 15, 17, 24, 31, 33, and 39 is non-obvious with respect to Owen, and it is respectfully requested that the rejection of claims 1, 8, 15, 17, 24, 31, 33, and 39 be withdrawn.

Claims 5-6, 12-13, 28-29, 37, and 42-43 depend respectively from, and further limit claims 1, 8, 24, 33, and 39. Thus, each of claims 5-6, 12-13, 28-29, 37, and 42-43 recites subject matter that is neither disclosed nor suggested in the cited art. Withdrawal of the rejection of claims 5-6, 12-13, 28-29, 37, and 42-43 is respectfully requested.

Claims 2, 9, 16, 18, 25, 32, 34, and 40 were rejected under 35 U.S.C. §103(a) as being allegedly unpatentable as obvious over Owen in view of Pond and further in view of U.S. Publication No. 2003/0023850 of Brown *et al.* ("Brown"). The Office Action acknowledged that the combination of Owen and Pond does not disclose or suggest all of the features of the claims. The Office Action, therefore, cited Brown to remedy the deficiencies of the combination of Owen and Pond. Applicants respectfully traverse this rejection.

Brown does not remedy the above-identified deficiencies of the combination of Owen and Pond. Claims 2, 9, 16, 18, 25, 32, 34, and 40 depend respectively from, and further limit, claims 1, 8, 15, 17, 24, 31, 33, and 39. Thus, the combination of Owen, Pond, and Brown does not does not disclose or suggest all of the elements of the rejected claims.

Brown generally relates to verifying messaging sessions by digital signatures of participants. Brown was cited in the Office Action as disclosing, for example, that "[t]the private key further encrypts a checksum determined for the contents log that is stored with the signature," quoting from paragraph [0049] of Brown. Even taken this quoted portion of Brown as a given for the sake of the argument, Brown would not (and does not) disclose the other five features discussed above with respect to the independent claims. Thus, Brown does not remedy the above-identified deficiencies of the combination of Owen and Pond and the combination of Owen, Pond, and Brown fails to disclose or suggest all of the elements of any of the presently pending claims. Thus, it is respectfully requested that the rejection of claims 2, 9, 16, 18, 25, 32, 34, and 40 be withdrawn.

Claims 7, 14, 23, 30, 38, 44 were rejected under 35 U.S.C. §103(a) as being allegedly unpatentable as obvious over Owen in view of Pond and further in view of U.S. Patent No. 6,557,044 of Cain ("Cain"). The Office Action acknowledged that the combination of Owen and Pond does not disclose or suggest all of the features of the claims. The Office Action, therefore, cited Brown to remedy the deficiencies of the combination of Owen and Pond. Applicants respectfully traverse this rejection.

Cain does not remedy the above-identified deficiencies of the combination of Owen and Pond. Claims 7, 14, 23, 30, 38, 44 depend respectively from, and further limit, claims 1, 8, 17, 24, 33, and 39. Thus, the combination of Owen, Pond, and Cain does not does not disclose or suggest all of the elements of the rejected claims.

Cain generally relates to method and apparatus for exchange of routing database information. Cain was cited in the Office Action as disclosing that "incremental checksumming may be utilized. Initially, the checksum for all routes in a set is computed by determining ," quoting from column 2, lines 64-67, of Cain. Even taken this quoted portion of Cain as a given for the sake of the argument, Cain would not (and does not) disclose the other five features discussed above with respect to the independent claims. Thus, Cain does not remedy the above-identified deficiencies of the combination of Owen and Pond and the combination of Owen, Pond, and Cain fails to disclose or suggest all of the elements of any of the presently pending claims. Thus, it is respectfully requested that the rejection of claims 7, 14, 23, 30, 38, 44 be withdrawn.

For the reasons set forth above, it is respectfully submitted that each of claims 1-2, 5-9, 12-18, 21-25, 28-34, 37-40, and 43-44 recites subject matter that is neither disclosed nor suggested in the cited art. It is, therefore, respectfully requested that all of claims 1-2, 5-9, 12-18, 21-25, 28-34, 37-40, and 43-44 be allowed, and that this application be passed to issuance.

If for any reason the Examiner determines that the application is not now in condition for allowance, it is respectfully requested that the Examiner contact, by telephone, Applicants' undersigned representative at the indicated telephone number to arrange for an interview to expedite the disposition of this application.

In the event this paper is not being timely filed, Applicants respectfully petition for an appropriate extension of time. Any fees for such an extension together with any additional fees may be charged to Counsel's Deposit Account 50-2222.

Respectfully submitted,

Peter Flanagan

Peter Flanagan
Attorney for Applicants
Registration No. 58,178

Customer No. 32294
SQUIRE, SANDERS & DEMPSEY LLP
14^{TH} Floor
8000 Towers Crescent Drive
Vienna, Virginia 22182-6212
Telephone: 703-720-7800
Fax: 703-720-7802

PCF:dlh

Enclosures: Petition for Extension of Time
Check No. 20883